# OFFICE OF THE STATE AUDITOR

## NETWORK SECURITY ENGINEER

**Posting Number 2021-07**

**SALARY RANGE (Grade 13) CSA224: $62,904.51 - $94,356.76 (Commensurate with experience)**

**GENERAL STATEMENT OF DUTIES:**

The Network Security Engineer's role is to plan, implement and secure the OSA's on premise and cloud networks. The Network Security Engineer gathers and reviews technical specifications and architects a secure network, performing network equipment upgrades with 3rd party vendors, as well as supporting network monitoring and threat detection.

The OSA consists of the Executive office, an Administration office and 4 regional locations and with total staff of approximately 250 individuals including mobile and work from home staff. In addition, the Network Security Engineer works collaboratively with IT staff, contractors, vendors, and with the Commonwealth's Executive Office of Technology Services and Security (EOTSS) on joint projects such as network connectivity, security and Cloud migration.

Please note that in response to COVID-19, OSA employees have the option of working from home (telecommuting) or working in an assigned office. At some point in the near future, employees will be expected to work 40% of their work week in office, with 60% telecommuting. Also, as a requirement of employment, all OSA employees are required to provide proof of COVID-19 vaccination, or provide a negative COVID-19 PCR test weekly in order to access offices or worksites.

**SUPERVISION RECEIVED:**

Receive supervision from the Assistant Director of IT Operations.

**SUPERVISION EXERCISED:**

No direct supervision exercised. Incumbent may exercise technical supervision on 1-3 contractor employees on projects or as needed basis.

**DUTIES AND RESPONSIBILITIES:**

- Design, plan and implement network technologies and improve computing capabilities as technology advances from on premise to cloud. Architects network solutions that support a hybrid environment.
- Lead cloud migration programs and initiatives in the areas of VNets, VPN, firewall, routing, circuits, security and related technologies.
- Stay current on recent and emerging cybersecurity treats. Research and recommend new technologies and methods to secure the computing environment.
- Detect and prevent network security threats. Analyze network traffic for anomalies that would indicate a security threat and take corrective action.
- Configure, maintain and administer perimeter security systems such as firewalls and Intrusion Detection Systems and network devices such as routers, wireless devices and switches.
- Develop, document and maintain Enterprise security policies and procedures. Implement and test network disaster recovery and incident response plans. Implement cybersecurity awareness training and measure program effectiveness.
- Escalate to the Network Manager and the Assistant Director of IT Operations on network issues, needs, and problems.
- Create an environment of knowledge retention through mentoring, documentation, network diagrams, trainings and demonstrations.

- Collaborate with IT staff and vendors and oversee projects such as infrastructure refreshes and migrations.
- Advanced support for Help Desk escalations. Respond and communicate security alerts and incidents.

**MINIMUM QUALIFICATIONS:**

The successful candidate will possess and/or demonstrate:

- Bachelor's degree in Computer Science or combination of formal technical training in cybersecurity or networking and a minimum of 5 years of appropriate experience.
- Strong analytical, organizational, and communication skills. Collaborates with peers, vendors, management and the business on IT projects.
- Strong technical knowledge of Azure cloud infrastructure connections, architecture, planning and design.
- Excellent troubleshooting and diagnostic skills with strong attention to detail. Ability to identify problems and propose improvements.
- Knowledge of NIST Special Publication 800-53, CIS Controls and related security frameworks.
- Strong technical knowledge of IP, TCP/IP, DNS, DHCP, firewall rules and routing.
- Experienced in the implementation and support of software defined networking and SD-WAN technologies.
- Working knowledge of network facilities and data processing techniques, of personal computer hardware and software, of network operating system and security software, and of performance monitoring and capacity management tools.
- Working knowledge in Active Directory, Email, Storage, Virtualization, Backup and Recovery technologies.
- High level of both oral and written communications skills including the ability to communicate complex technical information effectively to non-IT staff.
- Ability to perform scheduled maintenance, upgrades and emergency tasks outside of normal business hours (nights/weekends).

**PREFERRED QUALIFICATIONS:**

- Certifications from security, network system and software providers such as Cisco and Microsoft including Microsoft MCITP, Microsoft MCSE, CompTIA Security, CompTIA Cybersecurity Analyst, CompTIA Network or Cisco CCNA.
- Knowledge of the Commonwealth's Executive Office of Technology Services and Security (EOTSS) wide-area network (MAGNet), security policies and Commonwealth Enterprise systems.
- Knowledge of MS Hyper-V, MS System Center Configuration Manager (SCCM), Cisco, FortiGate, Office 365 (Exchange Online, OneDrive, SharePoint) and MS Azure cloud solutions (IaaS and PaaS).
- Knowledge of Project Management methodologies (Waterfall and Agile).

***No Phone Calls Please*:**
To apply, please send a copy of your resume to: OSA.applications@sao.state.ma.us when you apply, we invite you to submit a copy of the OSA's Voluntary Self Identification Form, with your resume.

The Office of the State Auditor is committed to providing equal employment opportunities. Employment actions such as recruiting, hiring, training, and promoting individuals are based upon a policy of non-discrimination. Employment decisions and actions are made without regard to race, color, gender, religion, age, national origin, ancestry, sexual orientation, gender identity and expression, disability, military status, genetic information, political affiliation, or veteran's status.